



電腦博士Mr.HIROSEの

ITこぼれ話

第17回

「パソコンの障害対策」

ITプランナー 廣瀬隆夫

日本列島は大陸からの日本海プレートと太平洋プレートがぶつかった位置にあり、昔から地震の巣と言われています。今の首都圏では、いつ地震が来てもおかしくないと専門家から指摘されると背筋が寒くなります。パソコンの中の重要書類をどのように災害から守っていくかは切実な問題です。今回は会社で使われているパソコンなどのシステムの安全対策についてお話をしたいと思います。

パソコンは災害に弱い

会社の電話機やコピー機は、かなり乱暴に扱っても壊れることはありませんが、パソコンは、それに比べると軟弱です。足を引っ掛けて電源コードが抜けただけで、今まで書いていた文書が全て消えてしまったという経験をされた方も多いと思います。地震でビルが倒壊したり、雷が落ちたりしたら、かなり大きなダメージを受ける覚悟が必要です。普通に使っていてもコンピュータウイルス、停電、ハード

障害、操作ミスなどでデータが失われたり、漏えいしたりする危険性が常にあります。パソコンには、水を満たしたゴム風船の中で金魚を飼っているような危うさがあります。

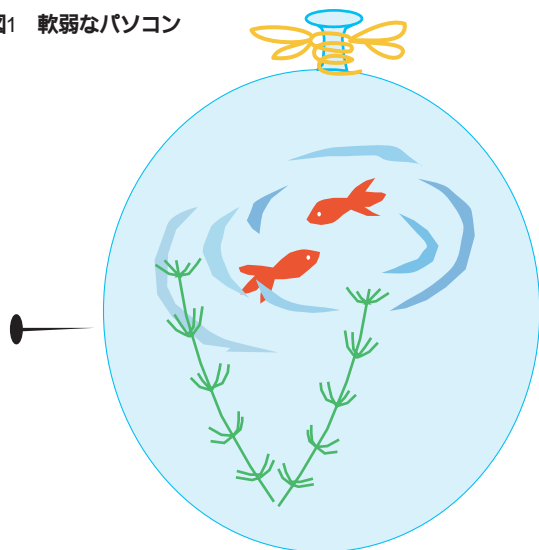
ファイルサーバによる安全対策

パソコンで電子メールを書いたり、見積もりを作ったりしていると、知らないうちにパソコンの中は書類だらけになってしまいます。このようなパソコンの管理を、日々の業務に追われながら行っていくのは辛いものがあります。最近は個人情報漏えいの問題でデータをフロッピーやMOディスクに落として保存しておくことが難しくなりました。そこで、電子的に安全な金庫を用意して、壊されたり、盗まれたくない重要な書類を入れるためのファイルサーバが導入されるようになりました。このサーバさえ管理しておけば、データは安全に保てます。

ハードディスクの信頼性を高める

サーバの中で、障害がもっとも起こりやすいのはハードディスクです。高速で回転する円盤に記憶されたデータを数マイクロンという間隙を保ちながら磁気ヘッドが読み取っていきます。書きこみ中に大きな震動が与えられたり、突然、停電になったりすると誤ったデータを書きこんでしまう危険性があります。また、円盤や磁気ヘッドの駆動部にはモータが使われていますので、モータの回転軸の磨耗などでハードディスクは、いつかは壊れる消耗品と考えたほうが良いでしょう。ハードディスクからキーンという異音が聞こえるようになったら要注意です。

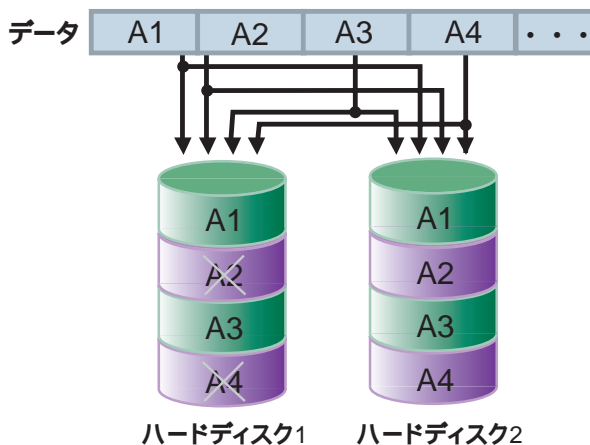
図1 軟弱なパソコン





このようなハードディスクの信頼性を高めるために、RAID（レイド）という構成を組むことができます。RAIDとは Redundant Arrays of Inexpensive Disksの略で別名ディスクアレイとも呼ばれています。複数のハードディスクに、データを分散して記録することで安全性を向上させています。一台のハードディスクが障害を起こしても、他の正常なディスクが補完してデータの修復をしてくれます。

図2 RAIDの仕組み



停電を監視する無停電装置

サーバの停電時の弱点を克服するためには無停電装置というものがあります。英語ではUPS (Uninterruptible Power Supply) と言います。この装置は思ったよりコンパクトで中に入っているバッテリーは5分程度の供給能力しかありません。これで長い停電でも大丈夫かと心配になりますが、無停電装置は停電を検知すると、サーバに信号を送り5分以内に安全にサーバの電源を切ってくれます。しかし、無停電装置に使われているバッテリーには寿命があり定期的な交換が必要です。台所に置いてある消火器の中身を数年毎に交換するのと同じことです。

ファイルサーバを何台か用意する

銀行のATMや駅の券売機が壊れているとイライラしますが、サービス全体が止まることはありません。これはファイルサーバでも同じで、重要なデータを格納しているサーバは何台か用意することで、システム全体の信頼性を上げることができます。ファイルサーバの待機の方法にはクールスタンバイとホッ

トスタンバイの2種類があります。クールスタンバイは予備機を用意して、壊れたら人が繋ぎ変える方法です。ホットスタンバイは、常に電源を入れておいて、どちらかのファイルサーバがダウンしたら自動的に切り替わるという方式です。24時間の安定稼働が必要な大規模なシステムで採用されています。

ファイルサーバのデータのバックアップ

ファイルサーバのデータは、最悪の事態に備えてバックアップを定期的に行う必要があります。手動で取る場合はCD-ROMやDVDなどが便利ですが、本格的なシステムでは、オーディオ用のカセットテープのような形をした大容量の高速ストリーマというものを使います。専用のソフトウェアを使うと、自動的に差分だけを定期的に保存させることができます。最近では、NAS (Network Attached Storage) サーバというLAN経由でファイルサーバのデータを自動的にバックアップしてくれる装置も普及しています。

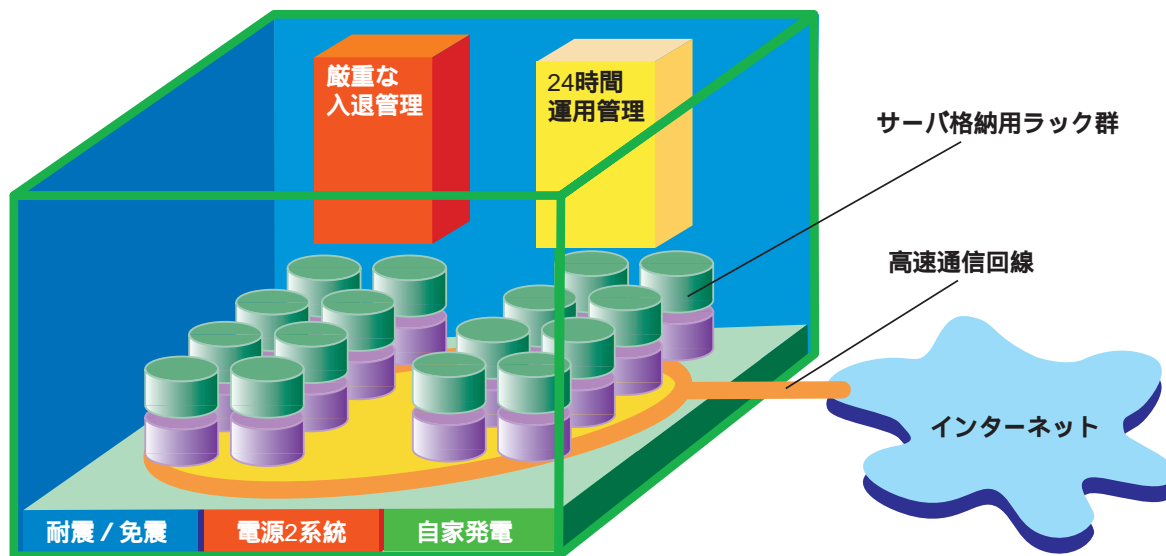
データセンターによる 障害対策

ネット証券や携帯電話サービスは止まってしまったら大変な営業損失につながります。また、不特定多数の人にサービスを提供するホームページの管理は、24時間の運用が必要なために自社では難しい場合があります。そこで、サーバの運用をデータセンターという専門業者に任せるという方法が考えられます。ニューヨークの世界貿易センタービルのテロ事件以降、データセンターの需要が増えてきています。

データセンターとは何か

データセンターは、サーバの運用に特化した要塞のような構造になっています。高速で信頼性の高いネットワーク、直下型地震でも倒壊しない耐震構造を持った堅牢な建物、自家発電装置や消火設備などが完備されています。また、入館時には、空港の荷物検査のような厳重なチェックが行われます。24時間365日の監視システムによるサーバの障害検知や障害が起こった時の復旧作業、夜中でもデータのバックアップができる体制もそろっています。

図3 データセンター



停電時の対策

データセンターは電力会社から複数系統で電力を供給されていたり、ビル全体の供給が可能なバッテリー、自家発電装置などを持っていますので、停電時にも業務が止まることはありません。

地震対策

データセンターは、ビルの構造自体が耐震や地震が来ても揺れにくい免震構造や壊れにくい耐震構造になっています。また、サーバが入るラックは倒壊防止対策が施されています。

サーバの稼働監視

システムを構成している機器やサービスが正常に稼働しているかを監視します。死活監視と言って、定期的にサーバに問い合わせをかけて反応があるかを調べ、トラブルの前兆を察知して障害を未然に防ぐことができます。

ネットワークの通信量の監視

平常時の閾値を著しく上回る通信量が発生したり、渋滞が起きている場合には、その原因を究明して、装置の修復をしたり、経路を変更したりしてネットワークを正常に戻します。

システムのリソース監視

システムリソースの監視では、ハードディスク、CPU、メモリなどのシステムの利用状況を確認します。ハードディスクの残容量などをチェックして常時、容量がギリギリの状態であれば、ハードディスクを増設するなどの処置を行います。

不正アクセス監視

ファイアウォールなどを導入して、システム全体のセキュリティを常にチェックしています。常に最新のセキュリティ対策が施されていますので、ハッカーによる不正アクセスやコンピュータウイルスの感染を防ぐことができます。

24時間オペレーションへの対応

ファイルサーバのデータのバックアップや個別業務オペレーションの代行が可能です。24時間人員が配置されているので、夜中の作業も任せることができます。

会社に導入されているパソコンのシステムは、肥大化と複雑化が進み重要度も増大しています。パソコンを会社の貴重な財産として位置づけ、個人まかせでなく、経営的な視点に立って運用管理していく必要があると思います。